COVER PAGE

Hewlett-Packard Docket Number:

200313427-1

Title:

SYSTEM AND METHOD FOR ACCESSING A WIRELESS NETWORK

Inventor:

Isaac Lagnado
8814 Sager Drive
Houston, Texas 77096

SYSTEM AND METHOD FOR ACCESSING A WIRELESS NETWORK

BACKGROUND

[0001] Wireless networks, such as wireless local area networks (LANs), have been developed to work in conjunction with or in place of wired networks, such as wired local area networks. For example, there are two basic types of wireless LANs – infrastructure and ad-hoc. In an infrastructure network, one or more wireless devices communicate directly with a base station or access point. The access point bridges the wireless LAN and a wired communication network and acts as a central controller for the wireless LAN. In an ad-hoc network, a LAN is created by the wireless devices themselves with no central controller. In an ad-hoc network, each device communicates directly with other devices in the network rather than through a central controller.

[0002] In a wireless network, air acts as the medium for data transmission. One of the concerns in a wireless network is that the medium over which data is transmitted is open and does not have the same constraints as a wired network. Malicious users can more easily access information traveling through the air. Furthermore, it is easier for malicious users to gain access to the wireless network. Existing wireless devices continually transmit probe requests to determine whether there are any wireless networks with which the wireless device can communicate. The probe request contains information about the type of network the wireless device desires to communicate with as well as information about the wireless device itself. Thus, the wireless device is "visible" to other wireless devices.

[0003] A malicious user of a wireless device can intercept these probe requests from other users (or wireless devices) and impersonate a wireless network with which the wireless device desires to communicate. An unsuspecting user (or wireless device) can unknowingly communicate with the impersonating wireless network, thereby enabling a malicious user to access information contained in the wireless device.

SUMMARY

[0004] In accordance with an embodiment of the present invention, a method for accessing a wireless network comprises detecting at least one wireless network within which a wireless device is located while the wireless device in a transmit off mode. The method also comprises determining whether the at least one wireless network is on a list of requested wireless networks.

[0005] In accordance with another embodiment of the present invention, a method for accessing a wireless network comprises automatically switching a wireless device to a transmit off mode in response to activation of the wireless device and detecting at least one wireless network within which said wireless device is located while the wireless device is in the transmit off mode.

[0006] In accordance with yet another embodiment of the present invention, a system for accessing a wireless network comprises a wireless device and application logic operatively associated with the wireless device. The application logic is adapted to selectively switch the wireless device between a transmit on mode and a transmit off mode based on an identification of at least one wireless network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0008] FIGURE 1A is a schematic diagram of an exemplary wireless local area network in which embodiments of the present invention may be used to advantage;

[0009] FIGURE 1B is a schematic diagram of another exemplary wireless local area network in which embodiments of the present invention may be used to advantage; and

[0010] FIGURE 2 is a flowchart of an exemplary method for accessing a wireless network in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0011] The preferred embodiment of the present invention and its advantages are best understood by referring to FIGURES 1 and 2 of the drawings.

[0012] FIGURE 1A is a schematic diagram of an exemplary wireless local area network (WLAN) 10 in which embodiments of the present invention may be used to advantage, and FIGURE 1B is a schematic diagram of another exemplary wireless local area network 20 in which embodiments of the present invention may be used to advantage. For convenience, the term "wireless network" is used herein to refer to any type of wireless network such as, but no limited to, a WLAN, a wireless wide area network (WWAN), or any other type of wireless network now known or later developed. Embodiments of the present invention are described below in connection with LANs (as illustrated in FIGURES 1 and 2); however, it should be understood that embodiments of the present invention may be used to advantage in any type of wireless network.

[0013] Wireless network 10 is an example of an infrastructure type wireless local area network, and wireless network 20 is an example of an ad-hoc type wireless local area network. Both networks 10 and 20 comprise a plurality of wireless devices 12, for example, a portable computer, a desktop computer, a cellular phone, a personal digital assistant (PDA), a camera, and/or the like. Wireless device 12 comprises a wireless network connectivity component, for example, a PCI (Peripheral Component Interconnect) card, USB (Universal Serial Bus), PCMCIA (Personal Computer Memory Card International Association) card, SDIO (Secure Digital Input-Output) card, NewCard, Cardbus, and/or the like, and is operable to communicate wirelessly with the aid of the wireless network connectivity component with a central controller or access point (AP) 14 or with other wireless devices 12. AP 14 is communicatively coupled with a communication network 16, such as the Internet, an Intranet, an extranet, and/or the like. AP 14 may be coupled with communication network 16 either wirelessly or with the aid of wires.

[0014] In an infrastructure network, such as wireless network 10, AP 14 coordinates communication between multiple wireless devices 12 within a predetermined range. The range depends on the wireless network standard being used for communication. The wireless network standard may be any standard now known or later developed, for

example IEEE 802.11 standard. In an ad-hoc network, such as wireless network 20, there is no central controller or AP 14 and wireless devices 12 communicate with each other directly rather than through the controller.

[0015] FIGURE 2 is a flowchart of an exemplary method 30 for accessing a wireless network in accordance with an embodiment of the present invention. At block 32, a wireless device, such as wireless device 12, is activated or switched on. At block 34, a transmit mode of the wireless device 12 is switched off so that the device 12 does not transmit signals. Wireless device 12 may be switched to a transmit off mode in response to a user request or action or may be automatically switched to a transmit off mode in response to or upon activation or another predetermined action or event. If desired, in an alternative embodiment, the transmit mode of the wireless device 12 may be set to an off state by default. In the transmit off mode, the device 12 is operable to receive signals from other devices or wireless networks but does not transmit any signals.

[0016] A wireless network periodically transmits a beacon frame that comprises a timestamp and attributes of the wireless network. In an infrastructure network, the beacon frames are transmitted by the access point, and in an ad-hoc network, the beacon frames are transmitted by other wireless devices operating within the ad-hoc network. At block 36, the wireless device 12 receives beacon frames from wireless networks within which the wireless device 12 is positioned. The receipt of the beacon frame aids the wireless device 12 in detecting wireless networks within which the wireless device 12 is located.

[0017] At block 38, a scan list of wireless networks is created based at least in part on the received beacon frames. The beacon frames include attributes, for example, an identifier, a media access control ID (MAC ID), a security level, network type, data rate, modulation scheme, and/or the like, of the wireless network. In an exemplary embodiment, the identifier comprises a service set identifier (SSID) associated with the corresponding wireless network. The scan list of wireless networks comprises attributes of the wireless networks from whom the beacon frames have been received. In an exemplary embodiment, the scan list comprises at least one of the following - an identifier, a MAC ID, a security level, network type, data rate, modulation scheme, and/or the like.

[0018] At block 40, the scan list is compared to a requested list of wireless networks. In an exemplary embodiment, the requested list is user-configurable and stored in

the wireless device 12. The requested list of wireless networks is a list of networks with which the user of the wireless device 12 is willing to associate. The requested list of wireless networks preferably comprises at least one of the following attributes of the wireless networks - an identifier, a MAC ID, a security level, network type, data rate, modulation scheme, and/or the like. In an exemplary embodiment, the requested list of wireless networks comprises both infrastructure networks and ad-hoc networks. If desired, the requested list of wireless networks may comprise only infrastructure networks or only ad-hoc networks.

[0019] At block 42, a determination is made as to whether any of the requested wireless networks are on the scan list. In an exemplary embodiment, this determination is made by comparing at least one attribute, for example an SSID, on the scan list and the requested list. In an exemplary embodiment, the determination is made by comparing a set of attributes on the scan list and the requested list. If none of the requested wireless networks are on the scan list, then the process starting at block 44 is executed. If at least one of the requested wireless networks is on the scan list, then the process starting at block 46 is executed.

[0020] At block 46, because there is a match in the requested wireless networks and the scanned wireless networks, a transmit mode of the wireless device 12 is switched on so that the wireless device 12 can transmit signals. In an exemplary embodiment, the wireless device 12 only transmits signals selectively, for example, when it has determined that it is within the range of a wireless network on its requested wireless networks list. Because the wireless device 12 transmits signals selectively, the probability of a malicious user impersonating a wireless network based on the information transmitted by the wireless device 12 and thereby creating a connection with the wireless device 12 through a rogue network is substantially reduced or eliminated. At block 48, a matched list of wireless networks that are on the scan list as well as the requested list is created. The list may be arranged in any desirable order. In an exemplary embodiment, the list is arranged based on a user defined priority as specified in the requested list.

[0021] At block 50, the wireless device 12 attempts to associate with the first wireless network on the matched list. In an exemplary embodiment, the wireless device 12 transmits an access request, for example, an association request frame, to the first wireless network on the matched list to request permission to associate with the wireless network.

After receiving an association request frame, the wireless network transmits an association response frame indicating the result of the association request. The association response frame is received by the wireless device 12. In an exemplary embodiment, after receiving the association response frame, the wireless device 12 initiates an authentication process with the access point. Any method for authentication now known or later developed may be used.

[0022] At block 52, a determination is made as to whether the association with the wireless network was successful. If the association with the wireless network was successful, then the process starting at block 54 is executed. If the association with the wireless network was not successful, then the process starting at block 56 is executed.

[0023] At block 56, a determination is made as to whether there are any more wireless networks on the matched list. If there are no more wireless networks on the matched list, then the process starting at block 44 is executed. If there are additional wireless networks on the matched list, then at block 58, the wireless device 12 attempts to associate with the next wireless network on the matched list, and the process starting at block 52 is executed.

[0024] At block 44, a determination is made as to whether the scan list contains any wireless networks that do not transmit an identifier. For example, some wireless networks transmit a beacon frame but do not include an identifier in the beacon frame for security reasons. Instead of the identifier, such wireless networks transmit a NULL string. Therefore, in an exemplary embodiment, at block 44, a determination is made as to whether the scan list contains any wireless networks with a NULL string as the identifier. If the scan list does not contain any wireless networks with a NULL string as the identifier, then the process starting at block 60 is executed.

[0025] If the scan list contains at least one wireless network with a NULL string as the identifier of the wireless network, then it is desirable that the user be informed about the existence of a wireless network whose identity is not known. Therefore, at block 62, the user is notified of the existence of the unidentified wireless network and prompted to select whether the user wants to attempt to associate with the unidentified wireless network. If the user chooses not to attempt to associate with the unidentified wireless network, then the process stating at block 60 is executed.

[0026] If the user chooses to attempt to associate with one of the unidentified or unknown wireless networks, then at block 64, a transmit mode of the wireless device 12 is switched on so that the wireless device 12 can transmit signals. In an exemplary embodiment, the wireless device 12 only transmits signals selectively, for example, when the user desires to attempt to associate with an unidentified wireless network. Because the wireless device transmits signals selectively, the probability of a malicious user impersonating a wireless network based on the information transmitted by the wireless device 12 and thereby creating a connection with the wireless device 12 through a rogue network is substantially reduced or eliminated.

[0027] At block 66, the wireless device transmits probe request frames to identify the unknown wireless networks. In response to receiving the probe request frames, the wireless network will transmit probe response frames. The probe response frame comprises information identifying the wireless networks transmitting the probe response frame, for example, an identifier, a MAC ID, a security level, network type, data rate, modulation scheme, and/or the like. The probe response frame is received by the wireless device 12. At block 68, a list of matched unknown networks is created. The list of matched unknown networks comprises a list of previously unknown networks that are also on the requested list of networks. In an exemplary embodiment, the list of matched unknown networks is created by comparing the identifiers received from the wireless networks with identifiers in the requested list of networks. The list may be arranged in any desirable order. In an exemplary embodiment, the list is arranged based on a user defined priority.

[0028] At block 70, the wireless device 12 attempts to associate with the first wireless network on the matched unknown networks list. In an exemplary embodiment, the wireless device 12 transmits an access request, for example, an association request frame, to the first wireless network on the matched unknown networks list to request permission to associate with the wireless network. After receiving an association request frame, the wireless network transmits an association response frame indicating the result of the association request. The association response frame is received by the wireless device 12. In an exemplary embodiment, after receiving the association response frame, the wireless device 12 initiates an authentication process with the access point. Any method for authentication now known or later developed may be used.

[0029] At block 72, a determination is made as to whether the association with the wireless network was successful. If the association with the wireless network was successful, then the process starting at block 54 is executed. If the association with the wireless network was not successful, then the process starting at block 74 is executed.

[0030] At block 74, a determination is made as to whether there are any more wireless networks on the matched unknown networks list. If there are no more wireless networks on the matched unknown networks list, then the process starting at block 60 is executed. If there are additional wireless networks on the matched unknown networks list, then at block 76, the wireless device 12 attempts to associate with the next wireless network on the matched unknown networks list and the process starting at block 72 is executed.

[0031] If the attempted association with a wireless network is successful at block 52 or block 72, then the process starting at block 54 is executed. The wireless device 12 may become disconnected from the wireless network due to a number of reasons, for example, de-authentication of the wireless network or wireless device 12, change of wireless device 12 configuration by the user, and/or the like. At block 54, a determination is made as to whether the wireless device 12 is still connected to the wireless network. If the wireless device 12 is not connected to the wireless network, then it is desirable to switch off the transmit mode of the wireless device 12. Therefore, the process starting at block 34 is executed.

[0032] At block 60, the user is prompted to select whether the user would like to start an ad-hoc network. If the user selects not to start an ad-hoc network, then the process starting at block 34 is executed. If the user selects to start an ad-hoc network, then at block 78, a transmit mode of the wireless device 12 is switched on so that the wireless device can transmit signals. In an exemplary embodiment, the wireless device 12 only transmits signals selectively, for example, when the user selects to start an ad-hoc network. Because the wireless device 12 transmits signals selectively, the probability of a malicious user impersonating a wireless network based on the information transmitted by the wireless device 12 and thereby creating a connection with the wireless device 12 through a rogue network is substantially reduced or eliminated.

[0033] At block 80, a determination is made as to whether the ad-hoc network should be discontinued. If the ad-hoc network is to be discontinued, then the process starting

at block 34 is executed. Otherwise, the wireless device operates within an ad-hoc network until the ad-hoc network is discontinued.

[0034] Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. The software, application logic and/or hardware may reside on wireless device 12. The application logic, software or an instruction set is preferably maintained on any one of various conventional computer-readable mediums. In the context of this document, a "computer-readable medium" can be any means that can contain, store, communicate, propagate or transport the program for use by or in connection with an instruction execution system, apparatus, or device.

[0035] If desired, the different functions discussed herein may be performed in any order and/or concurrently with each other. Furthermore, if desired, one or more of the above-described functions may be optional or may be combined without departing from the scope of the present invention.

[0036] A technical advantage of an exemplary embodiment of the present invention is that additional security is provided to the wireless device because the wireless device selectively transmits signals only upon the occurrence of certain events. Another technical advantage of an exemplary embodiment of the present invention is that a transmit mode of the wireless device may be switched off to prevent unauthorized access of the wireless device while the wireless device remains "on" or in an activated state.